безпекові ризики, але бажаючих бути фельд'єгерам не бракувало. Фельд'єгері мусили добре володіти зброєю, орієнтуватися у просторі, вміти поводитися з кіньми, полюбляти ризиковане життя, природу, свіже повітря. Окрім грошового забезпечення вони мали життя повне пригод. Разом з тим зазначимо, що поганий ризик-менеджмент керівників ДПУ регулярно призводив до загибелі фельд'єгерів, життя яких для більшовицької влади нічого не вартувало.

УДК 004.056.5 (355.4)

OSINT – ЕЛЕМЕНТ РОЗВІДКИ В УМОВАХ КІБЕРВІЙН

Максим Делембовський
Київський національний університет будівництва і архітектури
delembovskyi@knuba.edu.ua

Представлена тема присвячена використанню принципів OSINT (Open Source Intelligence) як елемента розвідки в умовах кібервійни. OSINT - це збір інформації з відкритих джерел, таких як соціальні мережі, веб-сайти, форуми тощо. В контексті кібервійни, OSINT може бути важливим інструментом для отримання інформації про цільову організацію або діяльність хакерів, що дозволяє розкрити слабкі місця і запобігти можливим атакам.

У представленій роботі розглядаються основні методи збору інформації через OSINT, а також приклади їх використання в кібервійні. Також розглянуті техніки захисту від збору інформації за допомогою OSINT. Заключній роботи присвячений перевагам використання OSINT в кібервійні і його місцю в загальній стратегії кібербезпеки.

Ця робота є корисною для кібербезпекових експертів, аналітиків, розвідників, а також будь-якої людини, яка цікавиться кібербезпекою і хоче дізнатися більше про використання OSINT в кібервійні.

Поняття OSINT виникло в наукових і дослідницьких колах ще в 1930-х роках в США, коли військові аналітики стали використовувати відкриті джерела для збору інформації про потенційних ворогів та їх діяльність. Однак, поняття OSINT стало більш популярним після завершення Холодної війни, коли з'явилася потреба в розвідці відкритих джерел, таких як мас-медіа, Інтернет, соціальні мережі та інші джерела відкритої інформації, для збору інформації про тероризм, кіберзлочинність та інші загрози національній безпеці.

У 1992 році в США було засновано Федеральне агентство з відкритої інформації (Federation of American Scientists), яке стало центром дослідження та розвитку методів збору, обробки та аналізу відкритої інформації. Пізніше, в 2001 році, в США було створено спеціальний орган для збору та аналізу інформації з відкритих джерел - Центр національної безпеки відкритої інформації (National Open Source Enterprise), який забезпечував збір, аналіз та передачу відкритої інформації різним агентствам та відомствам США.

У кінці 1990-х - початку 2000-х років з'явилися перші програми та інструменти для збору та обробки відкритої інформації. Наприклад, в 1996 році був

створений програмний продукт NetOwl, який використовується для збору та обробки відкритої інформації.

Станом на сьогодні існує безліч програмних інструментів для збору та аналізу відкритої інформації, а саме:

1. Maltego - це програма, яка дозволяє збирати та аналізувати інформацію про людей, організації та компанії з відкритих джерел.
2. Shodan - це пошукова система, яка дозволяє знаходити відкриті порти на мережі Інтернет та збирати інформацію про пристрої, які підключені до Інтернету.
3. Social Mention - це інструмент для моніторингу соціальних мереж, який дозволяє знаходити та аналізувати згадки про певні ключові слова або бренди в соціальних мережах.
4. Google Alerts - це безкоштовний сервіс від Google, який дозволяє налаштувати сповіщення про нову інформацію з відкритих джерел, яка містить певні ключові слова.
5. Hootsuite Insights - це інструмент для моніторингу соціальних мереж, який дозволяє відстежувати згадки про бренд або ключові слова в соціальних мережах, а також аналізувати поведінку аудиторії.
6. Tineye - це пошукова система, яка дозволяє знаходити зображення в Інтернеті, які мають аналогічний контент.
7. SpyFu - це інструмент для аналізу конкурентів у сфері цифрового маркетингу, який дозволяє дізнатися про платну та органічну пошукову оптимізацію, рекламні кампанії та ключові слова.

Це лише декілька з багатьох програмних інструментів для збору та аналізу відкритої інформації, які можуть бути використані для здійснення OSINT-дослідниками.

В нинішніх умовах військового стану України – це питання є досить актуальним так як постійно потребується робота над пошуком важливої розвідувальної інформації, пошуком колаборантів, військових злочинців та багато іншого. Відповідно цією роботою займаються як військові та правоохоронні органи так і громадські організації.

Для здійснення процесу пошуку інформації можна використовувати різні методи, а саме:

1. Пошук в Інтернеті - це найбільш очевидний метод збору інформації з відкритих джерел. Він може бути виконаний шляхом пошуку ключових слів та фраз в пошукових системах, включаючи Google, Bing, Yahoo! та інші.
2. Моніторинг соціальних мереж - цей метод дозволяє знаходити та аналізувати інформацію, яка опублікована в соціальних мережах, таких як Facebook, Twitter, LinkedIn, Instagram та інші. Це може бути корисним для збору інформації про людей, організації, події та багато іншого.
3. Аналіз відкритих джерел даних - цей метод включає в себе аналіз даних, які доступні з відкритих джерел, таких як газети, журнали, публічні бази даних, офіційні веб-сайти державних установ та інших організацій.
4. Застосування спеціальних програмних інструментів - для збору та аналізу відкритої інформації можуть бути використані спеціальні програмні інструменти, такі як Maltego, Shodan, Social Mention, Google Alerts та інші.

5. Співпраця з іншими джерелами - для збору інформації можна звертатися до джерел, таких як люди, експерти, співробітники організацій, які можуть надати корисну інформацію.

Ці методи можуть бути використані окремо або в комбінації з іншими методами для здійснення OSINT. Важливо також враховувати законодавство та етичний кодекс.

УДК 004.056.5

МЕТОД ДВІЙНОГО ХЕШУВАННЯ SHA З ДОДАТКОВИМ ПЕРЕБОРОМ

Денис Іванов
Київський національний університет будівництва і архітектури
denys.ivanov20@gmail.com

Метод двійного хешування SHA з додатковим перебором є ефективним і безпечним способом захисту інформації від несанкціонованого доступу. Даний метод використовує два послідовних хешування з використанням різних алгоритмів SHA, що дозволяє збільшити безпеку процесу.

Для підвищення безпеки методу, можна застосовувати додатковий перебір, який полягає у генерації випадкових значень та їх використанні у якості солі для хешування. Це дозволяє змінювати вихідний результат хешування для однакових даних, що унеможливлює зловмисникам відновлення вхідних даних.

Ще однією перевагою методу двійного хешування SHA з додатковим перебором є його швидкість та простота використання. Даний метод може бути використаний для захисту даних на різних рівнях, включаючи зберігання паролів та інших конфіденційних даних. Незважаючи на всі його переваги, метод двійного хешування SHA з додатковим перебором не є бездоганним. Існує можливість атаки методу шляхом зламування хеш-функцій, тому важливо регулярно оновлювати алгоритми хешування та солі для максимальної безпеки.

На сьогоднішній день методами локально чутливого-хешування (LSH) використовують майже у всіх сферах IT воно є досить актуальними. LSH – це метод, який знижую розмір багатомірних даних. Уявити апаратний або технічний засіб без використання LSH досить складно. Вони допомагають, знаходити дублікати, задіяні у кластеризації та конізації даних, знаходження найближчого сусіда, особливим представлення хешування є те що можна шифрувати в особистому коді інформацію. Для створення рекомендацій можуть використовуватися дані про дії користувача або його характеристики. У роботі розглядається задача кодування текстової інформації у хеш представлення та конізації даних. Представлення набору даних у вигляді LSH дуже важлива тому що саме цю методику використовують у збережені важливої інформації у базах даних, саме метод чутливого-хешування захищає нашу особисту інформацію від зловмисників.